IT & C

ISSN 2821 - 8469, ISSN – L 2821 - 8469, Volumul 2, Numărul 4, Decembrie 2023

Utilizarea IoT în războaiele moderne - Internetul Obiectelor Militare (IoMT)

Nicolae Sfetcu

Sfetcu, Nicolae (2023), Utilizarea IoT în războaiele moderne - Internetul Obiectelor Militare (IoMT), *IT & C*, **2**:4, 3-18, DOI: 10.58679/IT68691, https://www.internetmobile.ro/utilizarea-iot-in-razboaiele-moderne-internetul-obiectelor-militare-iomt/

Publicat online: 09.11.2023

Utilizarea IoT în războaiele moderne - Internetul Obiectelor Militare (IoMT)

Ing. fiz. Nicolae Sfetcu, MPhil[1]
nicolae@sfetcu.com

Abstract

The Internet of Things (IoT) has emerged as a disruptive technology with far-reaching applications in various sectors. In warfare, IoT is rapidly transforming the way militaries operate, communicate and gather information.

This essay explores the various applications of IoT in warfare, examining its impact on military strategies, logistics, and intelligence gathering. It also looks at the ethical and security considerations that arise as a result of this technological change.

Keywords: Internet of Things, IoT, Military Internet of Things, IoMT, Internet of Things Battles, IoBT, war

Using IoT in Modern Warfare - Military Internet of Things (IoMT)

Rezumat

Internetul obiectelor (IoT) a apărut ca o tehnologie disruptivă cu aplicații de anvergură în diferite sectoare. În război, IoT transformă rapid modul în care armatele operează, comunică și colectează informații.

Acest eseu explorează diversele aplicații ale IoT în război, examinând impactul acestuia asupra strategiilor militare, logisticii și colectarea de informații. De asemenea, analizează considerentele etice și de securitate care apar ca urmare a acestei schimbări tehnologice.

Cuvinte cheie: Internetul Obiectelor, IoT, Internetul Obiectelor Militare, IoMT, Internetul Obiectelor Bătăliilor, IoBT, război

---

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS)

IT & C, Volumul 2, Numărul 4, Decembrie 2023, pp. 3-18
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT68691
URL: https://www.internetmobile.ro/utilizarea-iot-in-razboaiele-moderne-internetul-obiectelor-militare-iomt/

Introducere

Internetul obiectelor (IoT) se referă la o rețea de dispozitive, senzori și sisteme interconectate care colectează, procesează și partajează date. Această tehnologie a revoluționat operațiunile militare, oferind o serie de beneficii, inclusiv comunicare îmbunătățită, analiza datelor în timp real și cunoaștere îmbunătățită a situației.

În timpul Războiului Rece, armata SUA a dezvoltat Sistemul de Supraveghere a Sunetului (SOSUS), o rețea de senzori acustici subacvatici, adică hidrofoane, plasate în Oceanul Atlantic și Pacific pentru monitorizări subacvatice[2]. DoD a contribuit la pregătirea terenului pentru viitoarele cercetări IoT la sfârșitul anilor 1960, prin crearea ARPANET[3].

În anii 1980, Agenția de Proiecte Avansate de Apărare (DARPA) a dezvoltat rețele de senzori wireless distribuite[4], în timp ce DoD a investit în miniaturizarea circuitelor integrate[5].

La finele anilor 1990, Departamentul Apărării a dezvoltat conceptul de război „centrat pe rețea” care a integrat domeniile fizic, informațional și cognitiv pentru a îmbunătăți schimbul de informații și colaborare[6]. Au fost astfel inițiate proiecte precum Nett Warrior[7], și Force XXI Battle Command Brigade și platforma de comunicare Below[8].

[2] Silicon Labs, „The Evolution of Wireless Sensor Networks”.
[3] Zheng și Carter, „Leveraging the Internet of Things for a More Efficient and Effective Military”.
[4] Silicon Labs, „The Evolution of Wireless Sensor Networks”.
[5] Zheng și Carter, „Leveraging the Internet of Things for a More Efficient and Effective Military”.
[6] Zheng și Carter.
[7] Malin, „U.S. Army’s Nett Warrior System Gets Future-Ready”.
[8] Defense Update, „Force XXI Battle Command Brigade and Below – FBCB2 - Defense Update”.

Începând cu 2019, cercetarea în tehnologia modernă IoT în domeniul militar a început să se dezvolte accelerat cu sprijin din partea Armatei, Marinei și Forțelor Aeriene ale SUA[9][10].

Acest eseu discută despre utilizarea cu mai multe fațete a IoT în război, subliniind impactul acestuia asupra strategiei, logisticii, informațiilor și preocupările asociate de etică și securitate.

Internetul obiectelor (IoT)

Internetul obiectelor (IoT) este format din dispozitive cu senzori, capacitate de procesare, software și alte tehnologii care conectează și schimbă date cu alte dispozitive și sisteme prin Internet sau alte rețele de comunicații[11].

IoT reprezintă convergența mai multor domenii interdisciplinare[12]: rețele, hardware încorporat, spectru radio, computere mobile, tehnologii de comunicare, arhitecturi software, tehnologii de detectare, eficiență energetică, managementul informațiilor și analiza datelor. Conform lui Paula Fraga-Lamas et al.[13], creșterea rapidă a IoT este condusă de patru progrese cheie în tehnologiile digitale. Primul este costul în scădere și miniaturizarea microelectronicilor din ce în ce mai puternice, cum ar fi traductoare (senzori și actuatoare), unități de procesare (de exemplu, microcontrolere, microprocesoare, SOC (System-on-a-chip), FPGA (Field-Programmable Gate Array)), și receptoare. Al doilea factor este ritmul rapid și extinderea conectivității fără fir. Al treilea este extinderea stocării datelor și a capacității de procesare a sistemelor de calcul. În cele din urmă, al patrulea este apariția aplicațiilor software și a analizelor inovatoare, inclusiv progrese în tehnicile de învățare automată pentru procesarea datelor mari. Aceste patru drivere sunt prezente în straturile stivei de tehnologie IoT. De exemplu, IoT poate include traductoare care colectează date despre condițiile fizice și de mediu. Aceste dispozitive transmit date prin cablu sau fără fir. rețeaua de comunicații către servere și computere care stochează și procesează date utilizând aplicații software și analize.Cunoștințele obținute din analiză pot fi utilizate pentru detectarea defecțiunilor, controlul, predicția, monitorizarea și optimizarea proceselor și sistemelor[14].

---

[9] Breeden II, „The Internet of Things' Role on Battlefields and at Sea".

[10] Beinart, „Air Force Improving Data Control, Cyber Security Before Deploying New Sensors For IoT Devices".

[11] Shafiq et al., „The Rise of "Internet of Things"".

[12] Miorandi et al., „Internet of Things".

[13] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety".

[14] Fraga-Lamas et al.

IoT oferă o perspectivă asupra comportamentelor umane, putând declanșa atenționări asupra proceselor de luare a deciziilor și permite factorilor de decizie militare să-și sporească cunoașterea situației operaționale, atenuând în același timp surpriza strategică. Utilizarea eficientă a IoT necesită o abordare bazată pe o teorie a identității și un concept clar al tipului de raționament logic pentru a răspunde nevoilor analitice, logica adecvării oferind o legătură conceptuală între interese, gândire, comportament și identitate. Pentru aceasta, este nevoie să se apeleze la cele trei tipuri de raționament logic, descrise în mod generic drept crowdsourcing, lucru de detectiv și proiectarea viitorului[15].

Impactul economic potențial al IoT va fi de la 3,9 trilioane de dolari la 11,1 trilioane de dolari pe an până în 2025[16].

Aplicații IoT în război

Utilizarea Internetului obiectelor (IoT) în război este un domeniu în evoluție rapidă, cu beneficii potențiale, dar și preocupări etice și de securitate semnificative. Iată câteva moduri în care tehnologia IoT este utilizată în război:

Comunicare îmbunătățită: IoT permite forțelor militare să mențină o comunicare fără întreruperi pe distanțe mari. Dispozitivele și senzorii conectați facilitează transmisia de voce, video și date, asigurând că trupele și comandanții pot rămâne în contact constant. Acest lucru îmbunătățește coordonarea, reduce timpii de răspuns și crește agilitatea operațiunilor militare.

Autentificare biometrică: IoT poate fi utilizat pentru autentificare biometrică și controlul accesului, asigurându-se că numai personalul autorizat poate accesa sistemele și datele militare critice.

Logistica și urmărirea activelor: IoT joacă un rol crucial în gestionarea lanțului de aprovizionare și în urmărirea activelor. Senzorii și etichetele RFID de pe echipamente și vehicule permit logisticii militare să urmărească inventarul în timp real, îmbunătățind alocarea resurselor și reducând riscul pierderii sau furtului echipamentelor. Această eficiență în logistică are un impact direct asupra succesului misiunii.

[15] Polyak și Ziemer, „The Internet of Things (loT) and the Art of Mapping a Population's Thinking, Behavior, and Influencers".

[16] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety".

IoT poate ajuta la optimizarea logisticii operațiunilor militare. Senzorii de pe consumabile și echipamente pot furniza date în timp real despre starea, locația și disponibilitatea acestora, permițând o gestionare mai eficientă a resurselor.

Echipamente pentru soldați: dispozitivele IoT sunt din ce în ce mai integrate în uniformele și echipamentele soldaților. Aceste obiecte purtabile pot monitoriza semnele vitale ale soldatului, pot oferi capacități de navigare și comunicare și pot îmbunătăți conștientizarea situației.

Sisteme fără pilot: dronele, vehiculele terestre fără pilot și alte sisteme autonome sunt echipate cu tehnologie IoT pentru a colecta informații, a efectua recunoașteri și a îndeplini diverse misiuni. Ele pot fi controlate de la distanță sau pot funcționa autonom.

Baze inteligente: bazele militare devin din ce în ce mai conectate și automatizate. Senzorii IoT sunt utilizați pentru securitate, managementul energiei și monitorizarea infrastructurii. Acest lucru sporește securitatea și eficiența instalațiilor militare.

Sisteme de arme la distanță: tehnologia IoT este integrată în sistemele de arme la distanță care permit operatorilor să controleze armele de la o distanță sigură. Aceste sisteme pot spori precizia și pot reduce riscul pentru soldați.

Senzorii și dispozitivele IoT pot fi utilizați pentru a urmări și monitoriza activele militare, cum ar fi vehiculele, armele și echipamentele, în timp real. Acest lucru le permite comandanților să aibă o mai bună cunoaștere a situației și să ia decizii mai informate.

Colectarea de informații: Colectarea și analiza informațiilor este o piatră de temelie a operațiunilor militare. Dispozitivele IoT, inclusiv drone, sateliți și senzori de la sol, oferă date în timp real despre mișcările inamicului, condițiile de mediu și dinamica câmpului de luptă. Aceste date ajută la luarea deciziilor și îmbunătățesc precizia acțiunilor militare.

Analiza datelor: datele generate de IoT pot fi procesate folosind analize avansate, permițând liderilor militari să ia decizii bazate pe date. De exemplu, datele de la diverși senzori pot fi folosite pentru a prezice nevoile de întreținere, pentru a detecta anomalii și pentru a evalua pregătirea generală a activelor militare.

Analiza logicii adecvării se întreabă care sunt comportamentele adecvate din punct de vedere normativ și etic, care depind de identitatea contextualizată. Analiștii derivă ipoteze

rezonabile și ipoteze de cercetare atunci când gama de comportamente acceptabile este cunoscută pe baza literaturii sociologice și antropologice existente[17].

Legătura dintre identitate, priorități și comportamente permite crearea unei matrice pentru a analiza modelele comportamentale din datele IoT, identificând modele de comportament și legând aceste comportamente cu o gamă de comportamente posibile legate de identități specifice.

Analiza IoT oferă o oportunitate exponențială emergentă de a dezvolta indicații și avertismentedintr-o perspectivă a identității și a logicii adecvării. Crowdsourcing-ul (raționament inductiv) urmărește să permită datelor să identifice corelații relevante, în timp ce tehnologia le poate spune analiștilor de ce trebuie să fie îngrijorați. Munca de detectiv (raționament deductiv) începe cu o ipoteză despre corelații și relații cauzale și apoi se uită la dovezi. Proiectarea viitorului (raționamentul abductiv) abordează problemele rele prin inferențele abductive.

Explorând populațiile prin cele trei lentile, IoT ar putea oferi date excelente pentru a determina ce viitor posibil este „în tendințe", având în vedere bogăția de date empirice, crowdsourcing, în timp ce munca de detectiv bună bazată pe bănuiala unui analist ar putea lumina o potențială amenințare localizată pe care crowdsourcing-ul. algoritmii ar putea să nu fie o tendință importantă. Sintetiza acestor tipuri de raționament este ceea ce face ca gândirea și comportamentul populațiilor să prindă viață[18].

Introducerea paradigmei Războiul Centrat în Rețea (NCW)[19] a transformat abordările militare tradiționale, integrând trei domenii: fizic, informațional, și cognitiv. Această paradigmă de conducere a dus la adoptarea tehnologiilor legate de IoT, utilizând tehnologiile COTS (Commercial Off-The-Shelf, produse comerciale standard), inclusiv telefoane inteligente comerciale sau identificarea prin radiofrecvență (RFID). Astăzi, acest concept este explorat în proiectele Uniunii Europene de cercetare precum RERUM, RELYonIt, FIESTA-IoT, BIGioT, bIoTope sau METIS-II[20].

Inteligența IoT poate fi oferită la trei niveluri: dispozitive IoT, noduri Edge/Fog și cloud computing[21]. Nevoia de control și decizie inteligentă la fiecare nivel depinde de sensibilitatea la

[17] Polyak și Ziemer, „The Internet of Things (loT) and the Art of Mapping a Population's Thinking, Behavior, and Influencers".
[18] Polyak și Ziemer.
[19] Tunnell, „[PDF] Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy | Semantic Scholar".
[20] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety".
[21] Mohammadi et al., „Deep Learning for IoT Big Data and Streaming Analytics".

timp a aplicației IoT. Integrarea algoritmilor avansati de învățare automată, inclusiv învățarea profundă, în dispozitivele IoT este un domeniu activ de cercetare, ajutate de analitica datelor IoT, extragerea informațiilor ascunse și predicția deciziilor de control. Învățarea automată este prezentă în IoT atât prin metode tradițional (regresia, mașina vectorială de suport) cât și avansate (rețelele neuronale convoluționale, LSTM și autoencoderul variațional)[22][23].

Impactul strategic al IoT în război: IoMT (IoBT)

{003} Internetul Obiectelor Militare (IoMT) este o rețea complexă de entități interconectate, sau „obiecte" cu beneficii recunoscute[24], care comunică între ele pentru a coordona, învăța și interacționa cu mediul pentru o gamă largă de activități într-un mod mai eficient și mai informat[25][26]. Ideea de bază este că că viitoarele bătălii militare vor fi dominate de inteligența mașinilor și războiul cibernetic[27].

Dispozitivele (”obiectele”) din IoMT posedă capacități fizice inteligente de detectare, învățare și acționare prin interfețe virtuale sau cibernetice integrate[28]. În general, dispozitivele IoMT formează o ”țesătură de date”[29] pentru *transport de date, captare a datelor, detectare și de acționare*, și un dispozitiv general cu capabilități de procesare și comunicare care poate face schimb de informații cu rețeaua mai mare[30]. S-a sugerat și posibilitatea de a încorpora în sistem obiecte neînsuflețite, cum ar fi plante și roci, prin dotarea acestora cu senzori care le vor transforma în puncte de colectare a informațiilor[31]. (e-Plants[32]).

Avantaje ale implementării IoMT:

- **Precizie și daune colaterale reduse**: IoT îmbunătățește precizia operațiunilor militare, reducând probabilitatea daunelor colaterale și a victimelor civile. Loviturile direcționate sunt mai precise, iar factorii de decizie au acces la informații în timp real care pot minimiza consecințele neintenționate ale războiului.

---

[22] Mohammadi et al.
[23] Mahdavinejad et al., „Machine learning for internet of things data analysis”.
[24] Silicon Labs, „The Evolution of Wireless Sensor Networks”.
[25] Rowlands, „The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare? | Australian Army Research Centre (AARC)”.
[26] Cameron, „Internet of Things Meets the Military and Battlefield”.
[27] Kott, Alberts, și Wang, „Will Cybersecurity Dictate the Outcome of Future Wars?”
[28] Kott, „Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments”.
[29] Sydney J. Freedberg Jr, „Project Rainmaker”.
[30] Russell și Abdelzaher, „The Internet of Battlefield Things”.
[31] Parker, „The Internet of Battlefield Things Is Coming. Are IT Pros Ready?”
[32] Saxena, „Researchers Create Electronic Rose Complete with Wires and Supercapacitors”.

- **Conștientizare îmbunătățită a situației**: Comandanții militari au acces la o mulțime de informații în timp real, permițându-le să ia decizii mai bine informate. IoT dă putere forțelor militare să înțeleagă mediul câmpului de luptă și să își adapteze strategiile în consecință.
- **Securitate cibernetică îmbunătățită**: Pe măsură ce armatele se bazează mai mult pe dispozitive interconectate, nevoia de măsuri solide de securitate cibernetică devine primordială. Vulnerabilitatea sistemelor IoT la atacurile cibernetice prezintă o provocare semnificativă care trebuie abordată pentru a proteja operațiunile militare.
- **Războiul informațional**: Manipularea și diseminarea informațiilor prin dispozitive și rețele conectate poate juca un rol semnificativ în războiul modern. Campaniile de dezinformare și propaganda sunt exemple ale modului în care tehnologia IoT poate fi utilizată pentru războiul informațional.

Scenarii pentru IoT critice pentru misiune[33]:

- *C4ISR*: Sistemele C4ISR folosesc milioane de senzori desfășurați pe o gamă largă de platforme pentru a oferi cunoaștere avansată a situației.
- *Sisteme de control al incendiului*: Implementarea end-to-end a rețelelor de senzori și a analizelor digitale permit răspunsuri complet automatizate la amenințările în timp real și oferă putere de foc cu precizie maximă.
- *Logistică*: Mai mulți senzori de nivel scăzut sunt deja utilizați în apărare, pentru monitorizarea și managementul flotei, sau rechizite individuale.
- *Operațiuni în orașe inteligente*: Infrastructurile IoT existente ar putea fi reutilizate în operațiuni militare.
- *Detecție personală, asistență medicală a soldaților și instruire a forței de muncă*: De exemplu, dispozitivele purtate pe corp[34], și monitorizări de fitness.
- *Colaborativ și crowd sensing*: Detecția colaborativă implică partajarea datelor de detectare între dispozitivele mobile, combinată cu comunicații robuste pe distanță scurtă.
- *Managementul energiei*: Reducerea cererii de energie din instalații prin investiții în proiecte de eficiență a instalațiilor sale.
- *Supraveghere*: Camerele și senzorii de securitate, combinați cu software-ul sofisticat de analiză a imaginilor și de recunoaștere a modelelor, ușurează monitorizarea.

Cerințe operaționale pentru IoMT[35]:

- Caracteristici de implementare
- Managementul și planificarea sistemului
- Servicii și aplicații acceptate
- Capabilități de rețea
- Topologii de rețea acceptate
- Capacități de mobilitate
- Capabilitati de securitate

[33] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety”.
[34] Cirani și Picone, „Wearable Computing for the Internet of Things”.
[35] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety”.

- Capacități de robustețe
- Capabilitati de acoperire
- Disponibilitate
- Fiabilitate
- Capabilitati de interoperabilitate
- Platforme țintă

Arhitectura IoT trebuie să țină cont de elementele de bază ale peisajului IoT 5 pentru a sprijini cerințele operaționale[36]:

- Protocoale standardizate IoT
  - Protocoale de nivel de aplicație
  - Protocoale de descoperire a serviciilor
- Tehnologii de activare
- Activarea protocoalelor
- Calcul
  - Platforme hardware și software
  - Platforme cloud
  - Fog Computing
- Analiza digitală {/002}

Programe implementate în IoMT:

Connected Soldier: susținut de Centrul de Cercetare, Dezvoltare și Inginerie Natick Soldier al Armatei SUA (NSRDEC), pentru crearea echipamentelor inteligente de corp[37].

Internet of Battlefield Things (IoBT): Înițiat în 2016, de U.S. Army Research Laboratory (ARL)[38] ca un plan detaliat pentru un război viitor prin o integrare a tehnologiei IoT în operațiunile militare[39]. Tehnologia IoBT încorporează inteligența predictivă, învățarea automată și rețelele neuronale[40].

Internet of Battlefield Things Collaborative Research Alliance (IoBT-CRA): Inițiat de ARL în 2017 pentru a avansa bazele teoretice ale sistemelor IoBT[41].

Mosaic Warfare: Un termen inventat în 2017, folosit de DARPA, pentru a descrie o abordare de „sisteme de sisteme” a războiului militar care se concentrează pe reconfigurarea

---

36 Fraga-Lamas et al.
37 Stackpole, „Keeping the Connected Soldier Connected with Simulation”.
38 Polit, „Army Takes on Wicked Problems With the Internet of Battlefield Things”.
39 Tucker, „US Army Seeks Internet-of-Battlefield-Things, Distributed Bot Swarms”.
40 Polit, „Army Takes on Wicked Problems With the Internet of Battlefield Things”.
41 Gudeman, „Next-Generation Internet of Battle Things (IoBT) Aims to Help Keep Troops and Civilians Safe”.

sistemelor și tehnologiilor de apărare[42]. Mosaic Warfare a fost promovat ca o strategie de a deruta și de a copleși forțele adverse prin desfășurarea unor sisteme de arme consumabile tehnologic, adaptabile, cu costuri reduse coordonate între ele, complicând procesul de luare a deciziilor pentru inamic[43].

System of Systems Integration Technology and Experimentation (SoSIT): Dezvoltat din Mosaic Warfare, un sistem de rețea care permite stații și platforme terestre care să transmită și să traducă date între ele[44].

Ocean of Things: Inițiat de DARPA în 2017, pentru a aplica tehnologia IoT la scară largă folosind tehnici analitice, pentru a stabili o conștientizare a situației maritime persistente pe zone mari oceanice[45], incluzând mii de flotoare mici, disponibile comercial, cu senzori care colectează date de mediu.

Provocări și preocupări

Utilizarea IoT în război ridică întrebări etice, în special în ceea ce privește confidențialitatea și potențialul de automatizare și armament autonom. Preocupările legate de supraveghere și confidențialitatea civilă, precum și de moralitatea desfășurării de arme complet autonome, necesită o analiză și o reglementare atentă.

În timp ce tehnologia IoT oferă multe beneficii potențiale pentru operațiunile militare, utilizarea sa în război ridică, de asemenea, preocupări etice și de securitate semnificative. Vulnerabilitățile dispozitivelor conectate fac sistemele militare susceptibile la atacuri cibernetice, iar colectarea de date extinse despre activitățile și personalul militar poate prezenta riscuri pentru confidențialitate și securitate. În plus, potențialul pentru arme autonome și implicațiile etice ale utilizării lor sunt subiecte de dezbatere internațională.

Integrarea IoT în operațiunile militare introduce noi riscuri de securitate. Hackerii și adversarii pot încerca să exploateze vulnerabilitățile sistemelor IoT, compromițând datele sensibile și eficiența militară. Protocoalele de securitate robuste sunt esențiale pentru a atenua aceste amenințări.

---

42 Magnuson, „DARPA Pushes 'Mosaic Warfare' Concept".
43 DARPA, „DARPA Tiles Together a Vision of Mosaic Warfare".
44 Hitchens, „DARPA's Mosaic Warfare - Multi Domain Ops, But Faster".
45 Barry, „DARPA & The Ocean of Things".

În războiul cibernetic, dispozitivele IoT sunt vulnerabile la atacuri cibernetice, iar exploatarea acestor vulnerabilități poate face parte dintr-o strategie mai largă de război cibernetic. Atacatorii pot viza sistemele și infrastructura militară conectate, perturbând comunicarea, supravegherea și operațiunile critice.

Principalele provocări și limitări tehnice în domeniul militar sunt evidențiate de Grupul operativ de cercetare al NATO (RTG) „Aplicații militare ale internetului obiectelor" (IST-147), și IST-ET-076, „Internetul obiectelor militare". Principalele preocupări miliare includ dependența de introducerea manuală, prelucrarea limitată a datelor, lipsa automatizării și arhitectura IT fragmentată[46]. Preocupările legate de securitate includ riscul atât de amenințări adverse, cât și de defecțiuni ale sistemului care ar putea compromite întreaga rețea[47]. Pe lângă riscurile de interferență digitală și manipulare de către hackeri, au fost exprimate și îngrijorări cu privire la disponibilitatea semnalelor wireless puternice în locații de luptă la distanță[48].

Securitatea este cea mai mare preocupare în adoptarea tehnologiei IoT[49]. Cele mai multe dintre preocupările de securitate sunt similare cu cele ale dispozitivelor convenționale[50], precum utilizarea unei autentificări slabe, uitarea de a schimba acreditările implicite, mesajele necriptate trimise între dispozitive, injecții SQL, atacuri Man-in-the-middle și gestionarea slabă a actualizărilor de securitate[51]. În plus, dispozitivele IoT au limitări operaționale severe în ceea ce privește puterea de calcul, astfel încât nu pot utiliza măsuri de securitate de bază (preum firewall, sau criptarea) care ar crește timpul de răspuns[52].

Există și riscul unor injectări de erori în sistem, neintenționat sau ca atacuri pentru a introduce defecte în sistem pentru a schimba comportamentul dorit[53].

Dispozitivele IoT accesibile la internet slab securizate pot fi, de asemenea, subminate pentru a ataca pe alții. În 2016, un atac distribuit de denial-of-service alimentat de dispozitive

---

[46] GAO, „Defense Logistics".
[47] MeriTalk, „DARPA Floats a Proposal for the Ocean of Things".
[48] Sternstein, „A more connected military means new battlefield glitches, too".
[49] Weissman, „We Asked Executives About The Internet Of Things And Their Answers Reveal That Security Remains A Huge Concern".
[50] Li și Xu, *Securing the Internet of Things*.
[51] Bastos, Shackleton, și El-Moussa, „Internet of Things".
[52] Liu et al., „Security and Privacy Challenges for Internet-of-Things and Fog Computing".
[53] Ahmadi, Kiaei, și Emamdoost, „SN4KE".

Internet of Things care rulează malware-ul Mirai a distrus un furnizor de DNS și site-uri web importante[54]. Mirai Botnet a infectat aproximativ 65.000 de dispozitive IoT în primele 20 de ore[55].

Internet of Things Security Foundation (IoTSF) a fost lansată în 2015 cu misiunea de a securiza Internetul obiectelor. În 2017, Mozilla a lansat Project Things pentru rutarea dispozitivelor IoT printr-un gateway sigur Web of Things[56]. La nivel de guverne se pot lua măsuri specifice de reglementare pentru a securiza dispozitivele IoT[57].

În ciuda încrederii în potențialul IoT, în prezent acesta se confruntă cu bariere în adoptarea tehnologiei IoT pe o scară mai largă. Mike Farley a susținut în Forbes că, deși soluțiile IoT atrag utilizatorii timpurii, fie le lipsește interoperabilitatea, fie un caz de utilizare clar pentru utilizatorii finali.[291] Un studiu realizat de Ericsson cu privire la adoptarea IoT în rândul companiilor daneze sugerează că mulți se luptă „să identifice exact unde se află valoarea IoT pentru ei”[58].

Datele IoT trebuie securizate cu o combinație de tehnologie blockchain, modificări ale hardware-ului sau prin construirea de aplicații cu securitatea ca o considerație principală.

Concluzie

IoT ar putea exacerba provocările cu care se confruntă analiștii în mediul informațional. Implicarea IoT necesită cercetare și analiză cu privire la motivațiile din spatele și implicațiile datelor primite pentru construcția socială a realității.

Integrarea IoT în război a revoluționat modul în care operează armatele moderne, îmbunătățind comunicarea, logistica și colectarea de informații. IoT oferă numeroase avantaje strategice, dar ridică și preocupări etice și de securitate importante. Pe măsură ce utilizarea IoT în război continuă să evolueze, este imperativ ca forțele militare și factorii de decizie să găsească un echilibru între valorificarea beneficiilor acestei tehnologii și atenuarea riscurilor asociate acesteia. Viitorul războiului va fi din ce în ce mai interconectat, solicitând o abordare cuprinzătoare pentru a aborda provocările și oportunitățile prezentate de IoT.

Implementarea mai largă a aplicațiilor IoT în apărare va necesita un timp mai îndelungat. Domeniul intelligence și cel al militar trebuie să adopte cele mai bune practici pentru dezvoltarea

[54] Woolf, „DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say”.
[55] Antonakakis et al., „Understanding the mirai botnet”.
[56] Francis, „Building the Web of Things – Mozilla Hacks - the Web Developer Blog”.
[57] Alfandi, Hasan, și Balbahaith, „Assessment and Hardening of IoT Development Boards | SpringerLink”.
[58] Ericsson, „Every. Thing. Connected. A study of the adoption of «Internet of Things» among Danish companies”.

tehnologiei și achizițiile din sectorul privat și ar trebui să ia în considerare un model de jos în sus de inovare și achiziții. Armata ar trebui să investească în dezvoltarea de noi tehnici de securitate care pot fi aplicate dispozitivelor și aplicațiilor COTS, inclusiv celor găzduite în cloud. Accentul ar trebui să se pună pe investiții în măsuri de securitate scalabile în loc să securizeze sisteme individuale. Această abordare le va oferi apărării și PS o pârghie mai mare în investițiile lor IoT, permițându-le venituri mai bune pe dolar cheltuit pe cercetare și dezvoltare proprie, exploatând în același timp potențialul militar IoT[59].

Implementarea IoT în război necesită o analiză atentă a acestor probleme etice, legale și de securitate pentru a asigura utilizarea responsabilă și sigură a acestei tehnologii în contexte militare.

Bibliografie

Ahmadi, Mohsen, Pantea Kiaei, și Navid Emamdoost. „SN4KE: Practical Mutation Testing at Binary Level". arXiv, 13 februarie 2021. https://doi.org/10.48550/arXiv.2102.05709.

Alfandi, Omar, Musaab Hasan, și Zayed Balbahaith. „Assessment and Hardening of IoT Development Boards | SpringerLink", 2019. https://link.springer.com/chapter/10.1007/978-3-030-30523-9_3.

Antonakakis, Manos, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, et al. „Understanding the mirai botnet: 26th USENIX Security Symposium". *Proceedings of the 26th USENIX Security Symposium*, Proceedings of the 26th USENIX Security Symposium, 2017, 1093–1110.

Barry, Mark. „DARPA & The Ocean of Things". *Aberdeen Strategy & Research* (blog), 21 decembrie 2017. https://www.aberdeen.com/featured/darpa-ocean-things/.

Bastos, D., M. Shackleton, și F. El-Moussa. „Internet of Things: A survey of technologies and security risks in smart home and city environments". În *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 1–7, 2018. https://doi.org/10.1049/cp.2018.0030.

Beinart, Matthew. „Air Force Improving Data Control, Cyber Security Before Deploying New Sensors For IoT Devices". Defense Daily, 24 aprilie 2018. https://www.defensedaily.com/air-force-improving-data-control-cyber-security-deploying-new-sensors-iot-devices/air-force/.

Breeden II, John. „The Internet of Things' Role on Battlefields and at Sea". Nextgov.com, 1 mai 2018. https://www.nextgov.com/ideas/2018/05/internet-things-role-battlefields-and-sea/147877/.

Cameron, Lori. „Internet of Things Meets the Military and Battlefield: Connecting Gear and Biometric Wearables for an IoMT and IoBT". IEEE Computer Society, 1 martie 2018. https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt/.

Cirani, Simone, și Marco Picone. „Wearable Computing for the Internet of Things". *IT Professional* 17 (21 septembrie 2015): 35–41. https://doi.org/10.1109/MITP.2015.89.

[59] Fraga-Lamas et al., „A Review on Internet of Things for Defense and Public Safety".

DARPA. „DARPA Tiles Together a Vision of Mosaic Warfare”, 2019. https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare.

Defense Update. „Force XXI Battle Command Brigade and Below – FBCB2 - Defense Update”:, 23 iulie 2005. https://defense-update.com/20050723_fbcb2.html, https://defense-update.com/20050723_fbcb2.html.

Ericsson. „Every. Thing. Connected. A study of the adoption of «Internet of Things» among Danish companies”, 2020. https://www.ericsson.com/49928a/assets/local/news/2015/11/every-thing-connected.pdf.

Fraga-Lamas, Paula, Tiago M. Fernández-Caramés, Manuel Suárez-Albela, Luis Castedo, și Miguel González-López. „A Review on Internet of Things for Defense and Public Safety”. *Sensors* 16, nr. 10 (octombrie 2016): 1644. https://doi.org/10.3390/s16101644.

Francis, Ben. „Building the Web of Things – Mozilla Hacks - the Web Developer Blog”. Mozilla Hacks – the Web developer blog, 2017. https://hacks.mozilla.org/2017/06/building-the-web-of-things.

GAO, U. S. Government Accountability. „Defense Logistics: DOD Has Addressed Most Reporting Requirements and Continues to Refine Its Asset Visibility Strategy | U.S. GAO”. Data accesării 8 noiembrie 2023. https://www.gao.gov/products/gao-16-88.

Gudeman, Kim. „Next-Generation Internet of Battle Things (IoBT) Aims to Help Keep Troops and Civilians Safe”, 2017. https://ece.illinois.edu/newsroom/news/3875.

Hitchens, Theresa. „DARPA’s Mosaic Warfare - Multi Domain Ops, But Faster”. *Breaking Defense* (blog), 10 septembrie 2019. https://breakingdefense.com/2019/09/darpas-mosaic-warfare-multi-domain-ops-but-faster/.

Kott, Alexander. „Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments”, 20 martie 2018.

Kott, Alexander, David S. Alberts, și Cliff Wang. „Will Cybersecurity Dictate the Outcome of Future Wars?” *Computer* 48, nr. 12 (decembrie 2015): 98–101. https://doi.org/10.1109/MC.2015.359.

Li, Shancang, și Li Da Xu. *Securing the Internet of Things*. Syngress, 2017.

Liu, Ximeng, Yang Yang, Kim-Kwang Raymond Choo, și Huaqun Wang. „Security and Privacy Challenges for Internet-of-Things and Fog Computing”. *Wireless Communications and Mobile Computing* 2018 (24 septembrie 2018): e9373961. https://doi.org/10.1155/2018/9373961.

Magnuson, Stew. „DARPA Pushes ‘Mosaic Warfare’ Concept”, 2018. https://www.nationaldefensemagazine.org/articles/2018/11/16/darpa-pushes-mosaic-warfare-concept.

Mahdavinejad, Mohammad Saeid, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, și Amit P. Sheth. „Machine learning for internet of things data analysis: a survey”. *Digital Communications and Networks* 4, nr. 3 (1 august 2018): 161–75. https://doi.org/10.1016/j.dcan.2017.10.002.

Malin, Carrington. „U.S. Army’s Nett Warrior System Gets Future-Ready”. *Armada International* (blog), 20 iulie 2023. https://www.armadainternational.com/2023/07/u-s-armys-nett-warrior-system-gets-future-ready/.

MeriTalk. „DARPA Floats a Proposal for the Ocean of Things”, 2018. https://www.meritalk.com/articles/darpa-floats-a-proposal-for-the-ocean-of-things/.

Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, și Imrich Chlamtac. „Internet of Things: Vision, Applications and Research Challenges". *Ad Hoc Networks* 10 (1 septembrie 2012). https://doi.org/10.1016/j.adhoc.2012.02.016.

Mohammadi, Mehdi, Ala Al-Fuqaha, Sameh Sorour, și Mohsen Guizani. „Deep Learning for IoT Big Data and Streaming Analytics: A Survey". *IEEE Communications Surveys & Tutorials* 20, nr. 4 (2018): 2923–60. https://doi.org/10.1109/COMST.2018.2844341.

Parker, Paul. „The Internet of Battlefield Things Is Coming. Are IT Pros Ready?" C4ISRNet, 3 octombrie 2018. https://www.c4isrnet.com/opinion/2018/10/03/the-internet-of-battlefield-things-is-coming-are-it-pros-ready/.

Polit, Kate. „Army Takes on Wicked Problems With the Internet of Battlefield Things", 2018. https://www.meritalk.com/articles/army-takes-on-wicked-problems-with-the-internet-of-battlefield-things/.

Polyak, Mark, și Katie Ziemer. „The Internet of Things (loT) and the Art of Mapping a Population's Thinking, Behavior, and Influencers". În *SMA White Paper - What Do Others Think and How Do We Know What They Are Thinking?* Mariah Yager, 2018. https://nsiteam.com/social/wp-content/uploads/2018/03/White-Paper_What-Do-Others-Think_March2018_FINAL.pdf.

Rowlands, Greg. „The Internet of Military Things & Machine Intelligence: A Winning Edge or Security Nightmare? | Australian Army Research Centre (AARC)", 2017. https://researchcentre.army.gov.au/library/land-power-forum/internet-military-things-machine-intelligence-winning-edge-or-security-nightmare.

Russell, Stephen, și Tarek Abdelzaher. „The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making". În *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, 737–42, 2018. https://doi.org/10.1109/MILCOM.2018.8599853.

Saxena, Shalini. „Researchers Create Electronic Rose Complete with Wires and Supercapacitors". Ars Technica, 1 martie 2017. https://arstechnica.com/science/2017/03/researchers-grow-electronic-rose-complete-with-wires-and-supercapacitors/.

Shafiq, Muhammad, Zhaoquan Gu, Omar Cheikhrouhou, Wajdi Alhakami, și Habib Hamam. „The Rise of "Internet of Things": Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks". *Wireless Communications and Mobile Computing* 2022 (3 august 2022): e8669348. https://doi.org/10.1155/2022/8669348.

Silicon Labs. „The Evolution of Wireless Sensor Networks", 2013. https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf.

Stackpole, Beth. „Keeping the Connected Soldier Connected with Simulation". Digital Engineering, 1 septembrie 2016. https://www.digitalengineering247.com/article/keeping-the-connected-soldier-connected-with-simulation.

Sternstein, Aliya. „A more connected military means new battlefield glitches, too". *Christian Science Monitor*, 2017. https://www.csmonitor.com/World/Passcode/2017/0331/A-more-connected-military-means-new-battlefield-glitches-too.

Sydney J. Freedberg Jr. „Project Rainmaker: Army Weaves 'Data Fabric' To Link Joint Networks". *Breaking Defense* (blog), 17 noiembrie 2020. https://breakingdefense.sites.breakingmedia.com/2020/11/project-rainmaker-army-weaves-data-fabric-to-link-joint-networks/.

Tucker, Patrick. „US Army Seeks Internet-of-Battlefield-Things, Distributed Bot Swarms”. Defense One, 18 iulie 2017. https://www.defenseone.com/technology/2017/07/us-army-seeks-internet-battlefield-things-distributed-bot-swarms/139533/.

Tunnell, C. D. „[PDF] Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy | Semantic Scholar”, 2014. https://www.semanticscholar.org/paper/Network-Centric-Warfare-and-the-Hierarchy-Tunnell/804eecfc51ef8c9f43cf4556a44d88bf4e2eff5f.

Weissman, Cale Guthrie. „We Asked Executives About The Internet Of Things And Their Answers Reveal That Security Remains A Huge Concern”. Business Insider, 2015. https://www.businessinsider.in/we-asked-executives-about-the-internet-of-things-and-their-answers-reveal-that-security-remains-a-huge-concern/articleshow/45959921.cms.

Woolf, Nicky. „DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say”. *The Guardian*, 26 octombrie 2016, sec. Technology. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

Zheng, Denise E., și William A. Carter. „Leveraging the Internet of Things for a More Efficient and Effective Military”, 17 septembrie 2015. https://www.csis.org/analysis/leveraging-internet-things-more-efficient-and-effective-military.